Firewall - What it is, why you need one, and safe default settings

Gridinsoft Help Center

What it is

Why it matters

Most attacks start with a connection from the outside - or a risky app calling out. A well-tuned firewall blocks malware, scans, and suspicious traffic while letting normal work continue.

How it works

- Rules & policies - allow known-good ports, block the rest
- Stateful inspection - track conversations so replies are allowed, fakes are not
- Next-gen features - app awareness, IPS, malware filtering, DNS controls

Good defaults

- On endpoints - enable the built-in OS firewall and block inbound by default
- On routers - close unused ports, disable remote admin from the internet
- For services - put apps behind a reverse proxy or WAF, and limit who can reach admin panels

Quick setup wins

- Start with deny by default - allow only what you need.
- Limit RDP/SSH/VPN to specific IPs - require MFA.
- Turn on logging and alerts - review new blocks weekly.
- Pair with DNS filtering and auto-patching for layered protection.
- Test from the outside - use a port scan to confirm nothing extra is open.